Industry Roundtable Report
SEPTEMBER 2026

DIGITAL PRODUCT PASSPORTS AND THE FUTURE OF MOBILE DEVICES

INDUSTRY ROUNDTABLE MOBILE DISRUPT 2026

Fontainebleau, Miami

Prepared By:

Peter C. Evans, PhD

Rich Bulger

ALL THINGS CIRCULAR apkudo

Industry Roundtable Report

This report provides an overview of the Industry Roundtable discussion held on July 6, 2026, at the Fontainebleau Resort in Miami, in conjunction with the Mobile Disrupt Conference. All conference participants were welcome to join the Roundtable discussion on the role of digital product passports and the future of the mobile industry. Discussions were held under the Chatham House Rule, meaning participants were free to use the information received, but neither the identity nor the affiliation of the speakers, nor that of any other participant, could be revealed.

The Industry Roundtable was hosted by Peter Evans and Rich Bulger of All Things Circular. We also acknowledge the participation of Jason Smith, Head of Services Partnerships at GSMA, who provided an overview of GSMA's Device homologation pilot project. We thank Apkudo for the support that made this report of the roundtable proceedings possible.

ALL THINGS CIRCULAR apkudo

Please cite as: Peter C. Evans, Digital Product Passports and the Future of Mobile Devices: Industry Roundtable Report, Denver, Colorado, September 2026.

Table of Content

Executive Summary ---- 03

Introduction ---- 04

What the Rountable Discussed ---- 04

Why Mobility Needs Digital Product Passports ---- 05

Regulatory Landscape ---- 06

Lessons from Identity Standardization: What Automotive's VIN Teaches Mobility ---- 07

Defining a Mobility DPP ---- 08

DPP vs. Trust Certificate ---- 09

Data Spaces: The Future Device Data Layer ---- 11

GSMA Device Homologation Pilot ---- 12

Building the Mobility Device Data Space Rulebook ---- 15

Implications for Secondary Markets and Circular Business Models ---- 16

Conclusion ---- 18

Executive Summary

On July 6, 2026, All Things Circular convened an industry roundtable at the Fontainebleau Miami Beach alongside the Mobile Disrupt Conference to address a pressing question for the mobility sector: how should stakeholders govern the data that will define every device's lifecycle by 2030?

The discussion brought together OEMs, carriers, marketplaces, refurbishers, recyclers, regulators, and financial services firms. It was informed by briefing material on secondary-market economics, the EU regulatory trajectory, and GSMA's device-homologation pilot.

Digital product passports (DPPs) are rapidly becoming an operating requirement, not simply a future compliance concern. The EU's Ecodesign for Sustainable Products Regulation will require DPPs for consumer electronics and frames them as governed, multi-party data systems—not standalone databases. At the same time, pre-owned devices have become a mainstream category, yet the industry still lacks a reliable, interoperable means to follow billions of devices through resale, repair, refurbishment, and end-of-life pathways.

Participants agreed that a DPP must be a continuous, trusted lifecycle record rather than a one-time certificate. The central challenge is governance: determining who may read, write, verify, report, and protect device data across organizational boundaries. The group favored federated data spaces over centralized databases, allowing data to remain with its source while sharing policy-controlled responses when needed. GSMA's device-homologation pilot, supported by OEMs, regulators and Apkudo's Device Passport™ Platform, was discussed as an initial step toward this model.

The opportunity for industry-led alignment is open but narrowing. Participants drew lessons from automotive's long path to VIN standardization while arguing that mobility can move faster, using existing GSMA IMEI and TAC infrastructure and a 2030 regulatory horizon. The roundtable demonstrated the value of cross-industry dialogue to build DPP systems that enable circular value while protecting legitimate commercial interests.

Introduction

By 2030, the mobile industry will operate on a fundamentally different data footing than it does today. Devices, such as phones, tablets, and laptops, will no longer move through opaque lifecycles punctuated by disconnected records. Instead, their identities, materials, ownership histories, performance, and end-of-life outcomes will be captured in governed digital product passports that span markets and business models. Regulators are shifting from static certification regimes to continuous, data-driven oversight, and secondary markets for smartphones are becoming central to industry economics rather than an afterthought. This more integrated, data-rich future cannot be established by any single company, association, or government. It must be built through collective effort across the mobility ecosystem.

Against this backdrop, an industry roundtable convened at Mobile Disrupt 2026 to explore how the mobility ecosystem should define the rules, trust mechanisms, and incentives that will govern digital product passports and the data spaces beneath them. The session brought together stakeholders from across the device lifecycle and secondary market: OEMs and carriers, marketplaces and refurbishers, regulators, investors and financial services firms, software and data platforms, logistics providers, and advisory and compliance specialists. The session opened with briefing material on market trends, the EU regulatory landscape, and the GSMA Device homologation pilot, then moved into facilitated discussion and live polling. This paper covers the briefing content and what participants discussed, debated, and voted on.

What the roundtable discussed

- A digital product passport is a governed, multi-party lifecycle accounting record, not a database or a one-time compliance certificate. Participants explicitly rejected the "birth-to-death certificate" framing as too static.
- DPP adoption is a governance problem before it is a technology problem. Success depends on clear answers to who can read, write, verify, report, and protect data, not on better data infrastructure alone.
- Participants are unlikely to contribute data without a neutral, trusted steward and clear commercial value. Data exposure, liability, and competitive risk were the top concerns; commercial value and neutral stewardship were the top incentives.
- Data spaces, not centralized databases, are the architecture participants see as viable. The GSMA Device homologation pilot, built on Apkudo's Device Passport™ Platform, was presented as early example of the steps that are needed to demonstrate how this model works in production.
- The industry has a narrow window to shape a common framework before DPPs arrive as fragmented, jurisdiction-specific mandates instead of a coherent, industry-led standard.

What Participants Told Us

Live Menti[1] polling during the Roundtable captured participant sentiment directly through an interactive app:

• In one word, a DPP should be: "transparent," "trust," "device history," "interoperable," "standardized," "trustworthy," "accurate," "comprehensive."

• Biggest concerns about contributing data: data exposure and privacy; liability for accuracy; losing control of the data; integration cost and effort; competitive risk; unclear commercial value.

• What would make participants contribute: clear commercial value; a neutral, trusted steward; regulatory certainty; assurance that competitors cannot see their data; low integration costs; proof that others will participate.

Taken together, these responses explain why the roundtable was needed. The industry recognizes the strategic necessity of digital product passports and accepts that the 2030 landscape will be passported. But participants were clear that the industry will only move decisively if governance, neutrality, and value creation are built into frameworks and pilots from the outset, not added afterward.

Why Mobility Needs Digital Product Passports

Briefing materials presented to the group made the case that digital product passports are becoming a practical necessity well before 2030, driven by two converging forces: regulation and market economics.

Market data presented at the roundtable underscored how quickly secondary markets have moved from the periphery to the center of mobility economics. According to IDC's Worldwide Used Smartphone Forecast, the global market for used smartphones, including officially refurbished and used devices, reached 309.4 million units in 2023, a 9.5 percent increase over 2022, and is projected to grow to 431.1 million units by 2027, an 8.8 percent compound annual growth rate. IDC values that 2027 market at $109.7 billion.[2] Pre-owned is no longer a niche transaction category. It is a mainstream consumer choice, and the data shows it compounding.

1. Menti (Mentimeter) is a platform for building interactive presentations, letting a presenter run live polls, quizzes, word clouds, and Q&A that audience members answer in real time from their own devices.

2. IDC press release, "Worldwide Market for Used Smartphones Is Forecast to Surpass 430 Million Units with a Market Value of $109.7 Billion in 2027" (January 22, 2024)

Figure 1. Device Lifecycle States

Lifecycle analysis briefed to the group showed that of the 1.34 billion smartphones sold worldwide in 2022, roughly 1.03 billion followed informal disposition paths: stored as backup devices, kept for privacy or sentimental reasons, given to friends or family, or disposed of as general waste. Only about 310 million went through formal take-back, refurbishment, resale, or material recovery channels. Without a mechanism like a digital product passport to track events across both formal and informal flows, the industry cannot reliably quantify, let alone optimize, circular value creation. [3]

This changes what it means to manage devices (see Figure 1). Tier 1 players (OEMs and carriers), Tier 2 marketplaces and refurbishers, and Tier 3 recyclers and material recovery firms operate as distinct actors in the device lifecycle, each serving a different function as devices move from first sale through resale to end-of-life. But their outcomes are linked: OEMs and carriers realize residual value and deliver on circular commitments only as devices flow successfully through Tier 2 and Tier 3.

When these actors make lifecycle data available, trust increases and value creation is distributed across the chain. When data remains siloed and non-standard, grading inconsistency, fraud, and gray-market opacity erode margins and confidence at every tier.

Regulatory landscape

The EU's Ecodesign for Sustainable Products Regulation (ESPR) was briefed as the reason digital product passports are inevitable for consumer electronics by 2030.[4] ESPR and the European Commission's Joint Research Centre DPP methodology define what an effective passport must provide: a governed, multi-party data system, not a single database of product

3. Peter C. Evans and Seth Heine, "Not Circular Enough! The World Needs to Double Smart Phone Reuse and Recycling by 2030," All Things Circular, 2025.

4. The legal basis for the DPP is the Ecodesign Regulation (ESPR) (EU) 2024/1781. For more general information and timelines for implementation see: https://single-market-economy.ec.europa.eu/single-market/digital-product-passport_en#what-is-a-digital-product-passport-dpp

facts. Five governance foundations were presented to the group:

- Data ownership and stewardship: clear accountability for creating, maintaining, and validating passport data.
- Role-based access control: defined rules for who can read, write, update, and report passport information.
- Trusted data infrastructure: secure integrity, authenticity, and availability across the product lifecycle.
- Interoperability and standardization: common data models and formats for exchange across stakeholders and borders.
- Lifecycle persistence: data that remains accessible across owners, service providers, marketplaces, and end-of-life actors.

ESPR treats the DPP as a distributed system of governance. It separates data management, access rights, and registry functions so that no single entity controls all passport data, and it explicitly rejects a single centralized database in favor of distributed data management with registries focused on discoverability and trust. For mobility, this means success requires neutral governance structures capable of managing permissions, trust, and lifecycle data across OEMs, carriers, marketplaces, repair providers, recyclers, and regulators, not just an internal IT project or a government registry. ESPR mandates DPPs at the product level, and by implication, data spaces and rulebooks at the ecosystem level.

Lessons from Identity Standardization: What Automotive's VIN Teaches Mobility

The roundtable looked to automotive's long transition from inconsistent vehicle identifiers to the standardized Vehicle Identification Number (VIN) for two lessons, one about what identity standards make possible and one about speed.

The first lesson is that identity infrastructure shapes market structure. Before VIN standardization, identifiers varied by manufacturer, plant, and jurisdiction, which made registration harder, theft easier to conceal, recalls more difficult, and cross-border trade friction-heavy. Once the industry converged on the 17-character VIN and aligned it with global manufacturer identifiers under ISO 3780, vehicle identity became interoperable, and an entire ecosystem of services followed: marketplaces that could match buyers and inventory, valuation tools that could price vehicles with confidence, lenders and insurers that could underwrite based on consistent data, and regulators that could run recalls with precision. A trusted identifier reduced information asymmetry and let markets scale around a shared

understanding of each asset. But a VIN only ever identified a vehicle; it said nothing about condition, history, or current state. Mobility DPPs must go further, treating the passport as a permissioned, multi-party record of lifecycle events, not just an identifier, so that a device is legible across its life, not merely identifiable at a point in time. [5]

The second lesson is about time, and it is a cautionary one rather than a template. Automotive's path from fragmented serial numbers to a fully standardized, cross-border identifier took decades: FMVSS 115 in 1968 established basic identification requirements, the 17-character VIN was not mandated until the 1981 model year, and the rules were not fully consolidated into federal code until 1996. Participants were direct on this point: mobility should not accept that timeline as a model.

The VIN's slow standardization reflected a period before shared digital infrastructure, common data protocols, and coordinated industry bodies existed to accelerate consensus. Mobility has GSMA, existing IMEI and TAC infrastructure, and a regulatory deadline already in view for 2030. With coordinated industry collaboration, standardization can and should happen in years, not decades. [6]

Defining a Mobility DPP

Roundtable participants discussed how to define a DPP in precise terms and to distinguish it from simpler notions that miss the point of lifecycle data and governance. There was consensus on the definition of a digital product passport. It is a continuously maintained, tamper-evident lifecycle record that captures significant events in a device's journey, from raw materials and design through manufacture, sale, activation, in-life use, repair, refurbishment, resale, and responsible end-of-life processing. Each event is recorded as a dated entry in the passport, like a stamp in a travel document, enabling the product's lifecycle to be understood as a sequence rather than a static snapshot.

The passport is issued at the beginning of a product's life and maintained throughout its use, repair, reuse, and recovery phases. Its information should remain accurate, traceable, and available to authorized parties for as long as required under applicable product, data-protection, and record-retention rules. At end of life, the passport can record verified recycling or other responsible final-treatment outcomes.

The roundtable distinguished static data, information that defines the product (identity, materials and origin, compliance and certificates), from dynamic data, information that changes over time (ownership and custody, battery health, repair and refurbishment history, usage diagnostics). Static data must be

5. Roman Rak, Dagmar Kopencova, and Miroslav Felcan. "Digital vehicle identity–Digital VIN in forensic and technical practice." *Forensic Science International: Digital Investigation* 39 (2021): 301307.

6. Peter C. Evans, "From VINs to Digital Product Passports: What Automotive Standardization Teaches the Mobile Industry, and Where It Can Go Further," *Platform Professional*, Substack, July 5, 2026.

accurate and durable; dynamic data must be captured in a way that is timely, trustworthy, and proportionate to the use cases it serves. If static fields are wrong, the passport's identity layer fails. If dynamic events are missing or unverifiable, the passport cannot support grading, warranty, insurance, finance, or ESG reporting with confidence.

The governance briefing framed the core challenge directly: a digital product passport is not a technology problem, it is a governance problem. Governance questions were organized around five action items, which recur throughout this paper and throughout the roundtable's discussion of both the DPP concept and the GSMA pilot:

- *Read*: who can see which parts of the passport, in what contexts.
- *Write*: who can add or update events, under what credentials and roles.
- *Verify:* who validates data (test labs, OEMs, regulators) and how assurance is signaled.
- *Report*: who can see aggregates and analytics derived from passport data.
- *Protect*: how sensitive information is secured, masked, or kept off-passport entirely.

Participants agreed that a DPP's value is not created by collecting more data. It is created by sharing the right data with the right people at the right time, under rules that all participants understand and trust.

DPP vs. Trust Certificate

A final distinction participants made is between the DPP itself and the Trust Certificate. The DPP is the complete lifecycle accounting record, built to serve every participant across the value chain and to support compliance, reporting, governance, and traceability. Its job is to be accurate, complete, and governed.

The Trust Certificate is a customer-facing proof generated from DPP data: a selective, verifiable snapshot of key facts designed to inspire confidence at the point of sale. In the roundtable materials, a Trust Certificate example for a resold iPhone 11 answered the questions a next-purchaser actually has: does it work, has the data been erased, is the battery healthy, has it been repaired, what condition is it in, and can the seller be trusted. It answers "yes, with evidence" by exposing verified functionality, verified data erasure, verified battery health, verified device status (carrier, lock, and blacklist checks), verified cosmetic condition, and verified chain of custody.

The DPP captures the history; the Trust Certificate complements it, turning lifecycle data into buyer confidence, faster purchase decisions, fewer returns, and higher resale values. If the DPP's underlying records are weak, the certificate can only offer superficial assurance.

If governance around what flows into the certificate is poorly designed, sensitive information could leak. Separating the lifecycle ledger from the commercial incentive layer, and governing both through shared standards, is what lets the ecosystem align circular business models, compliance, and customer trust without conflating deep data management with point-of-sale experience.

As illustrated in Table 1, The Digital Product Passport provides the governed lifecycle evidence; the Trust Certificate translates selected, verified evidence into a point-of-sale assurance for the next purchaser.

Table 1. DPP vs. Trust Certificate

Dimension	Digital Product Passport	Trust Certificate
Market focus	OEMs, carriers, repairers, refurbishers, marketplaces, recyclers, regulators, and authorized service providers	Next purchaser, reseller, marketplace, and warranty provider
Scope	Full product history and relevant lifecycle data	Selective facts relevant to the transaction
Data model	Continuously maintained, traceable, permissioned record	A generated, time-specific attestation
Core purpose	Compliance, traceability, reporting, circular operations, and governance	Buyer confidence, faster decisions, lower perceived risk
Example content	Product identity, materials, repair events, test history, custody events, compliance information, recovery outcomes	Functional test passed, battery health, data erasure verified, condition grade, lock/blacklist status
Access	Role- and policy-governed	Public or buyer-facing, with controlled verification

Data Spaces: The Future Device Data Layer

There was general agreement that by 2030, the architecture underpinning mobility DPPs cannot be a bigger database. It must be a governed data space: a federated environment in which participants share verifiable answers, not raw datasets, under rules they collectively define and control. Participants agreed with this framing over the course of the session, returning to one point in particular: the hardest problems in DPP adoption are not technical, they are governance problems.

A data space is a dynamic, federated, decentralized data infrastructure in which participants share data insights, not data copies, governed by machine-readable policies they define and control. Unlike a data lake or centralized registry, a data space leaves data physically where it belongs, with its original owner. What travels across the network is not the data itself but a policy-governed response to a specific, authorized query. In the airport-gate analogy used in the briefing, the gate verifies that a ticket is valid and lets the traveler through, but never downloads their entire travel history. It sees precisely what it needs and nothing more.

The practical contrast is between a centralized model, where uploading data effectively surrenders ownership to a registry operator, exposes competitive intelligence, and creates a single point of breach, and a data space, where ownership and sovereignty stay with the data provider, only query-specific answers are returned, access policies are enforced mathematically before any response, and there is no central repository to compromise. This same contrast underpins the GSMA Device homologation pilot described below, which the roundtable treated as the clearest available proof that the model works.

Roundtable polling on this topic returned to the same concerns and incentives noted earlier: data exposure and competitive risk as the top barriers, and a neutral, trusted steward paired with clear commercial value as the top drivers of participation. Participants were explicit that this is not a case of either party acting irrationally. Regulators genuinely need reliable device identity data, and OEMs genuinely cannot expose bulk production data without commercial harm. A governed data space is designed to resolve that tension by architecture rather than by promise.

GSMA Device Homologation Pilot

The GSMA Device Homologation Pilot was introduced to the roundtable as a concrete application of the data-space model to one of mobility's most challenging problems: how regulators and OEMs can share device identity data to combat counterfeits and enforce market entry rules without exposing sensitive commercial information. GSMA has partnered with Apkudo to provide the underlying data-sharing environment using its Device Passport™ Platform for this pilot. [7]

Homologation is the formal process by which a device is confirmed to meet national technical, safety, and legal requirements before it may be sold or operated on a domestic network. Every market has its own requirements, and homologation bottlenecks can delay launch dates, strand inventory in bonded warehouses, and erode the 90-day revenue peak that flagship devices depend on.

Device homologation and device attestation operate at different layers of the assurance model; see Table 2. Homologation asks whether a device model, type, or—where national rules require it—an individual device meets the applicable technical, legal, and network-entry requirements. It produces a regulatory or network approval, such as a certificate or type approval. Device attestation asks whether a specific device can be verified as associated with the claimed OEM and represented status at the time of

Table 2. Device Attestation vs Homologation

	Attestation	Homologation
Primary Value	Establishes confidence in the identity, provenance, integrity, and current verified status of a specific device	Establishes that a device model and/or individual device meets applicable technical and regulatory requirements
Authority	An OEM-originated assertion that authorized parties can independently verify under the scheme's identity, credential, and policy framework	Regulators, certification bodies, and mobile network operators
When it occurs	Repeated as needed during the device lifecycle or at an authorized point of verification	Once at the model or device level, before market entry
Core question	"Is this specific device associated with the claimed OEM and in the verified status represented at this point in time?"	"Is this *type* of device approved by regulators for use on this network or in this market?"

7. GSMA, "From fragmentation to control: why device manufacturers need an industry-led approach to homologation," Atlanta, July 6, 2026, https://www.gsma.com/newsroom/article/from-fragmentation-to-control-why-device-manufacturers-need-an-industry-led-approach-to-homologation/

inquiry. It produces a verifiable, device-level assertion without requiring the OEM to disclose its underlying production dataset. Homologation has historically occurred at the model or type level, though regulators increasingly apply device-level checks. Device attestation can be performed repeatedly throughout the device lifecycle whenever an authorized party needs to verify a specific IMEI or related device attribute. The GSMA pilot is deliberately scoped to IMEI-level device attestation: it returns a policy-governed result on whether the queried IMEI is associated with the claimed OEM and a valid TAC allocation, while building on the existing homologation regime for model-level approval.

Regulators rely on the IMEI, a unique 15-digit identifier assigned to every mobile device, to verify legitimate manufacture and approval. Counterfeiters have industrialized IMEI fraud, most commonly by cloning a legitimate, approved IMEI from a genuine device and assigning it to an unapproved or substandard device, which then passes basic network checks. Regulators need more granular, trustworthy IMEI data. OEMs treat their IMEI datasets as core intellectual property, since a sufficiently large dataset reveals production volumes, regional allocations, launch timing, and confidential commercial arrangements.

Why bulk IMEI sharing creates a trust gap

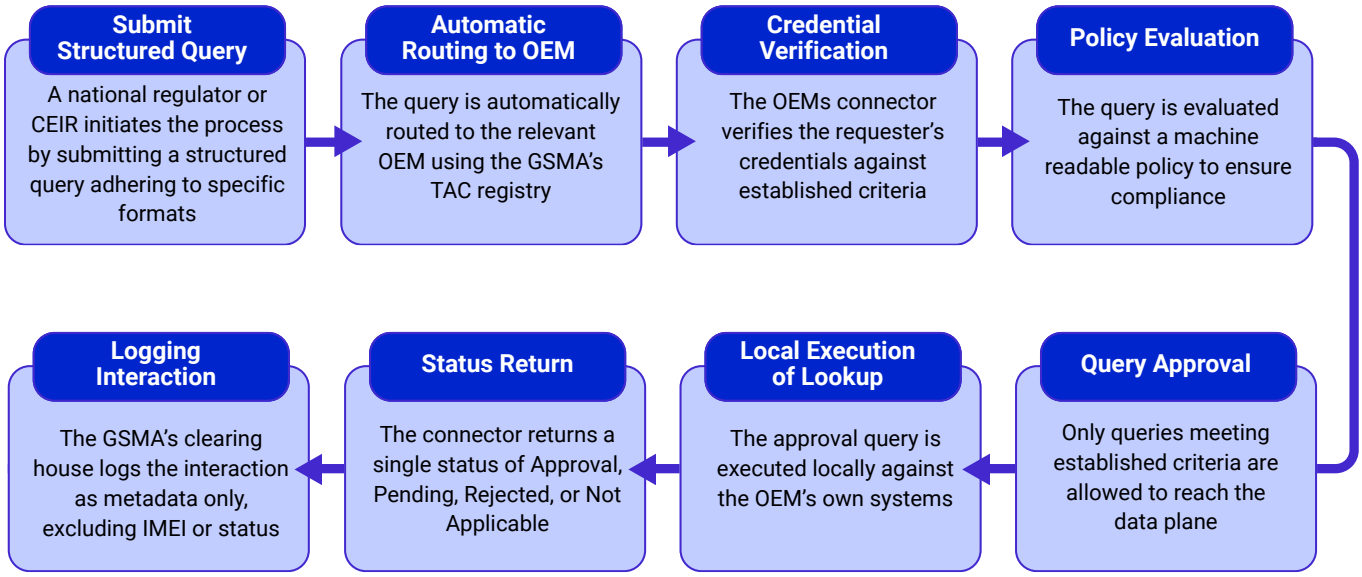
Bulk sharing proposals such as ITU-T Q.5057 envisaged OEMs uploading unencrypted IMEI datasets, paired with device specifications and target market identifiers, into centralized government registries. A bulk IMEI list is a precise, time-stamped map of an OEM's global production strategy. Revealing it, even to a registry with ostensibly secure controls, creates competitive risk OEMs uniformly reject. Centralized architecture compounds the problem: once uploaded, the OEM loses downstream visibility, there is no reliable way to audit access or revoke it, and a single breach exposes every participating manufacturer's production data. The result is a genuine trust gap, not a solvable-by-goodwill problem: regulators cannot combat IMEI cloning without reliable identity data, and OEMs will not provide that data in a form that exposes their commercial interests.

The Device Passport™ data-space approach

The Device Passport is a policy-governed, query-only data object that answers the regulator's binary question, does this IMEI belong to an approved device, with a verifiable yes or no, without exposing a single row of production data. It sits within a data-space architecture grounded in the International Data Spaces Association Reference Architecture Model and the Dataspace Protocol. GSMA serves as convening authority, scheme owner, and participant-credential issuer, while Apkudo provides the operational connector infrastructure linking OEM systems to the network.

The query path works as follows: a national regulator or CEIR submits a structured query; it routes automatically to the OEM that owns the relevant TAC range using GSMA's TAC registry; the OEM's connector checks the requester's verifiable credentials and evaluates the query against machine-readable policy; only approved queries reach the data plane; the lookup executes locally against the OEM's own systems, with no data leaving the OEM domain; the connector returns a single device-attestation result—such as approved, pending, rejected, or not applicable—and nothing else; and

Figure 2. Query Path for National Regulators and CEIR Submissions



GSMA's clearing house logs the interaction as metadata only, without storing the IMEI or the status. Production volumes, pricing, contract terms, PII, and inventory positioning are structurally outside the schema and cannot be queried.

Pilot scope: staged device-attestation levels

The pilot defines three progressive levels of device attestation that can support homologation and market-enforcement workflows. The pilot currently underway with GSMA is scoped to Level 1 only: determining whether a queried IMEI is associated with the claimed OEM and a valid TAC allocation.

Level 1, now being tested, answers the foundational question: Is the queried IMEI associated with the claimed OEM and a valid TAC allocation?

This level avoids full lifecycle mapping and minimizes integration complexity, making it easier for OEMs and regulators to join and validate the approach end to end. Level 2 extends to device association, confirming the IMEI is bound to a device of the expected model and configuration. Level 3 introduces jurisdiction-specific compliance, such as SAR limits or band support, with a status scoped to the querying market. Across all three levels, the pattern holds: regulators submit structured queries, OEM connectors evaluate the authorized query, relevant device-attestation criteria, and applicable policy, lookups run locally, and only minimal, status-level answers cross the boundary.

Pilot roles and neutral stewardship

The Homologation Data Space Rulebook defines the roles that make the pilot work and preserve neutrality. GSMA acts as scheme owner and oversight body: it defines the rules, admits participants, arbitrates disputes, and operates the clearing-house audit log. It also serves as the participant credential issuer, issuing and governing the verifiable credentials used to authenticate organizations and authorize data-space interactions. OEMs are data providers, owning and selectively exposing or revoking access to their data through connectors that enforce their own policies. Regulators and CEIRs are data consumers, submitting policy-authorized queries limited to specific types and jurisdictions. Apkudo operates as infrastructure service provider, deploying and running connectors that read from OEM systems under OEM-defined policies and enforce those policies in real time, without owning the data. This role separation is what participants described as the neutral, trusted steward they said was essential to their willingness to contribute data.

Building the Mobility Device Data Space Rulebook

The GSMA pilot and the roundtable discussion both point to the same destination: a functioning market-layer data space by 2030 in which DPPs live, queries flow across the ecosystem, and data sovereignty is preserved. Getting there is primarily a governance and participation challenge, one that needs to be codified in a shared Rulebook. Participants considered the International Data Spaces Association (IDSA) Rulebook[8] framework as a template for what a Mobility Device Data Space Rulebook would need to define.

- Scheme ownership and oversight: the body that owns the rules, admits participants, and arbitrates disputes. GSMA is the natural candidate, building on its role as global administrator of TAC and IMEI allocation.

- Participant roles: OEMs as data providers and authoritative sources of device-attestation results; regulators and CEIRs as authorized data consumers; GSMA as scheme owner, participant credential issuer, TAC-registry administrator, and clearing-house operator; and infrastructure vendors such as Apkudo as connector operators.

- Access and usage policies: machine-readable rules, not contractual promises, specifying permitted query types, jurisdictions, rate limits, time windows, and purpose constraints, evaluated by each connector before any response.

- Data interoperability model: a shared DPP data model and a common lifecycle vocabulary, such as the smartphone event taxonomy discussed at the roundtable, spanning pre-market, in-life, and end-of-life events, so terms like "approved" or "battery health" mean the same thing across connectors and jurisdictions.

8. International Data Spaces Association, IDSA Rulebook, Dortmund, Germany,2023, https://internationaldataspaces.org/idsa-rulebook/

- Onboarding and connector certification: how participants apply, how identity is verified and credentials issued, and how connectors are certified for correct protocol behavior and policy enforcement before they are trusted on the network.

- Legal and regulatory alignment: the contractual baseline every participant signs, and explicit compliance mapping to GDPR, the EU Data Act, ESPR, and homologation rules in each jurisdiction.

- Identity and trust framework: who issues, validates, rotates, and revokes participant credentials, so that each query and response is authenticated, authorized, and auditable rather than relying solely on an IP address or API key. Where required by the use case, device-attestation results should also be cryptographically authenticated and independently verifiable.

Participants framed the path to a mobility DPP ecosystem as a collective action problem with three pillars: standards and governance, which the Rulebook addresses directly; industry cooperation, since a DPP is only beneficial if OEMs, carriers, marketplaces, refurbishers, recyclers, regulators, insurers, and financiers all participate, rather than each regulator solving data sharing its own way; and economic incentives, since polling showed commercial value and neutral stewardship as the top factors that would make participants willing to contribute. The Rulebook explains how to participate; incentives explain why it is worth doing.

Positioned for 2030, a functioning device data space would support governed queries across several high-value use cases participants discussed: homologation workflows and IMEI-level device-attestation queries, including near-real-time responses where the participating systems and policies support them; verified resale and circular marketplaces using Trust Certificates to translate lifecycle data into buyer confidence; warranty and financing underwritten on verified condition and usage; loss recovery through federated blacklisting without exposing personal data; and ESG and regulatory reporting generated from DPP events with minimal manual data collection. In each case, data stays with its source, only policy-governed answers travel the network, and every interaction is logged for accountability.

Implications for Secondary Markets and Circular Business Models

The roundtable's secondary supply-chain mapping showed an ecosystem, Tier 1 OEMs and carriers, Tier 2 aggregators and wholesalers, Tier 3 refurbishers and retailers, plus logistics, software, testing, and finance enablers, that already moves hundreds of millions of devices per year but still struggle with grading inconsistency, fraud, and gray-market opacity. Tier 1 players are the first point of return but often do not share grading standards downstream. Tier 2 aggregators provide liquidity but frequently lack the automation and standardized grading needed to serve higher-paying customers. Tier 3 refurbishers and retailers operate closest to the end customer but have limited visibility beyond the point at which devices leave Tier 2.

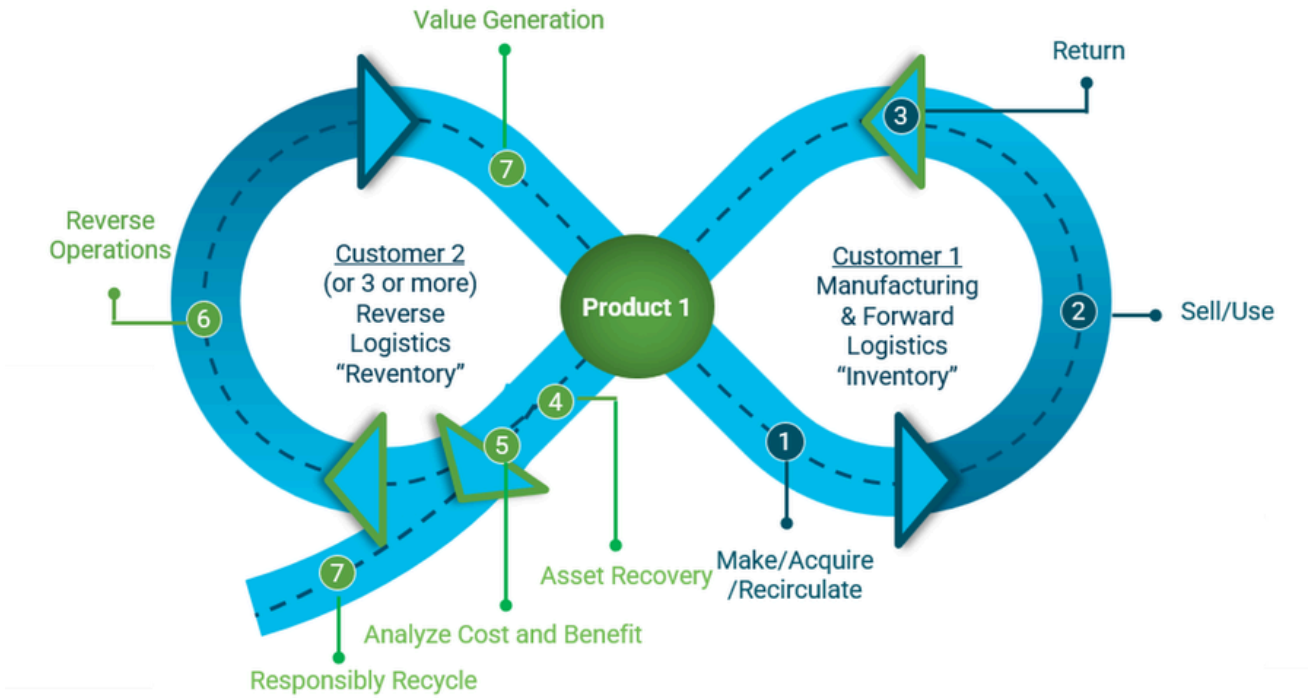
A DPP-enabled data space addresses these challenges in three ways that participants discussed directly. First, standardized lifecycle events give grading a common, data-driven language instead of relying on subjective assessment. Second, IMEI-level device attestation makes it harder for counterfeit, cloned-

identity, or improperly represented devices to enter secondary channels. Policy-governed blacklist checks can complement that process by identifying devices reported lost, stolen, or otherwise restricted. Third, federated custody and ownership events make it possible to trace where a device has been and whether its path aligns with authorized programs, reducing gray-market opacity. None of this requires any participant to surrender bulk datasets or commercially sensitive information.

The roundtable's "Product lifecycle Loop" framing distinguished the traditional sales model, focused on moving Customer 1 from Product 1 to Product 2, from the circular model, focused on moving Product 1 from Customer 1 to Customer 2, 3, and beyond. A DPP instruments that circular loop directly: each lifecycle event, manufacture, sale, use, repair, return, refurbishment, resale, and end-of-life, is captured as a stamp, so reverse-logistics operators can decide whether a device should be refurbished, resold, harvested for parts, or sent to material recovery based on verified history rather than heuristics. That, in turn, is the foundation for circular KPIs, such as reuse rates, average device age at resale, and repair-versus-replacement ratios, that can be tied directly to ESG commitments.

As discussed earlier in this paper, Trust Certificates are what convert this lifecycle data into commercial value at the point of sale: higher resale values for devices with verified functionality, erasure, and battery health; fewer returns and disputes from clearer pre-sale disclosure; and better-priced warranties and financing from insurers and lenders working off verified condition rather than assumption. As ESPR's DPP mandate comes into force and secondary smartphone markets continue to grow, IMEI attestation and device passports will not just be compliance tools. Participants were clear that they see this as the infrastructure on which circular business models, trusted marketplaces, and credible ESG reporting will be built.

Figure 3. Product Lifecycle Loop



Conclusion

Digital product passports emerged from the Mobile Disrupt 2026 industry roundtable as an imminent operating requirement for mobility, driven by ESPR and related standards on one side and the rapid expansion of secondary smartphone markets on the other. By 2030, every device will need a governed, multi-party lifecycle record. The real choice for the industry, as participants framed it, is whether DPPs arrive as fragmented, jurisdiction-specific mandates or as a coherent, industry-led framework grounded in shared standards and governed data spaces.

The roundtable helped define what that framework must be: a lifecycle accounting record linking static identity and materials data to dynamic events such as ownership transfers, repairs, diagnostics, and end-of-life outcomes, governed by clear rules for who can read, write, verify, report, and protect data. It pointed to the GSMA Device homologation pilot as evidence that IMEI attestation and data-space architecture are already moving into production, not remaining theoretical. And it anchored these architectural concepts in circular economics, showing how Tier 1, Tier 2, and Tier 3 actors depend on shared lifecycle data to reduce grading inconsistency, fraud, and gray-market opacity, with Trust Certificates as the commercial layer that turns lifecycle truth into buyer confidence and higher residual values.

Participants were consistent on one final point: industry participation will hinge on neutral stewardship, clear commercial value, regulatory certainty, and safeguarded data, not on regulatory pressure alone. A Mobility Device Data Space Rulebook, anchored by GSMA and informed by the homologation pilots running on the Apkudo Device Passport Platform, offers a practical way to meet those conditions. Unlike automotive's decades-long path to a standardized identifier, mobility already has the coordinating infrastructure and the deadline in view. The window to shape this framework, and with it the future of mobility data, is open now.

About the Authors

Peter C. Evans is a globally recognized expert on digital platforms and corporate strategy. He is Managing Partner at All Things Circular, a leading business development organization and platform advisory services firm. Peter has over 25 years of experience leading teams in identifying, framing, assessing, and communicating high-priority marketplace trends and disruptions that support business planning and investment prioritization. He has held senior strategy roles at large global enterprises, including KPMG and General Electric, and he also has extensive experience advising startup companies. He is a lifetime member of the Council on Foreign Relations and served on the board of the National Association for Business Economics. He is co-chair of the MIT Platform Strategy Summit and serves as an advisor to Marketplace Risk. He writes The Platform Professional, a popular Substack and teaches popular masterclass on the circular economy. His articles have appeared in Forbes, MIT Sloan Management Review, and academic journals. Peter received his BA from Hampshire College and his master's degree and PhD from MIT.

Rich Bulger is a recognized leader in reverse logistics, recommerce, and circular-economy business strategy with more than two decades of experience building and scaling sustainable product-recovery programs. He is Co-Founder of All Things Circular, a business development organization and platform advisory services firm focused on circular-economy innovation, eco-friendly product-transfer strategies, device trade-in, asset recovery, and secondary markets for used electronics. Rich has held senior leadership roles at major global enterprises, including Verizon and Cisco, where he led teams across operations, marketing, and reverse logistics. During his 17-year tenure at Verizon, he spearheaded the company's first in-store handset trade-in program in 2009. The program grew into a business generating approximately $1.6 billion annually from used-handset sales. At Cisco, he managed global reverse-logistics operations and supported supply-chain performance recognized through Gartner's Top Supply Chain rankings. Rich has contributed to the reverse-logistics profession as an advisory board member of the Reverse Logistics Association. His leadership foundation includes service in the U.S. Army, and he holds a master's degree in Reverse Logistics Management.

About All Things Circular, GSMA and Apkudo

All Things Circular, LLC

All Things Circular is a circular economy advisory, education, and media firm. We help companies turn reverse logistics, secondary markets, and circular operations into competitive advantage. We offer advisory services, masterclasses, training, research, and podcasting, with a focus on platform strategy, take-back programs, resale, reuse, recovery, and practical business transformation. To learn more, visit All Things Circular.

GSMA and GSMA Foundry

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

The GSMA Foundry is the Home of Mobile Innovation. We're the go-to hub for cross-industry collaboration and business development, where GSMA members rapidly develop real-world solutions, nurture new ideas, and scale proven solutions globally to shape our digital future. To learn more about the GSMA and the GSMA Foundry visit GSMA.

Apkudo

Apkudo is the Device Passport™ Platform for the connected device ecosystem. We capture and unify data from every program, transaction, and touchpoint across a device's lifecycle, creating a single, trusted Device Passport™ for every asset. For companies that manage, sell, or buy devices, this means a verified record they can act on: to restore buyer confidence, maximize value, and reduce risk at every decision point. To learn more, visit Apkudo.

All Things Circular, LLC

https://allthingscircular.com/

Apkudo

https://www.apkudo.com/